#34

Attorney Docket No.: 80410.0009

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

MOSKOWITZ, Scott, et al

Appl. No.: 08/999,766

Filed: July 23, 1997

For: STEGANOGRAPHIC METHOD AND DEVICE

Art Unit: 2132

Examiner: MEISLAHN, D.

MAIL STOP: Appeal Brief - Patents
Honorable Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REPLY BRIEF

Applicant hereby submits its Reply Brief pursuant to 37 C.F.R. § 1.193(b). Applicant believes no fees are required to file this response. However, if any fees are required with the filing of this response, Applicants respectfully request that any such fees be charged to Deposit Account No. 50-1129.

Respectfully submitted,

WILEY REIN & FIELDING LLP

Date: December 1, 2003

By: Floyd B. Chapman

Floyd B. Chapman, Reg. No. 40,555

WILEY REIN & FIELDING LLP
Attn: Patent Administration
1776 K Street, N.W.
Washington, D.C. 20006
Telephone: 202.719.7000
Facsimile: 202.719.7049

Attorney Docket No.: 80410.0009

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

MOSKOWITZ, Scott, et al

Appl. No.: 08/999,766

Filed: July 23, 1997

For: Steganographic Method and Device

Art Unit: 2132

Examiner: MEISLAHN, D.

Honorable Commissioner for Patents
Mail Stop: Appeal Brief-Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

REPLY BRIEF

Pursuant to 37 C.F.R. § 1.193(b), Appellant respectfully submits this reply brief to address the points of argument raised in the Examiner's Answer, mailed October 1, 2003.

ARGUMENT REGARDING REJECTIONS UNDER 35 U.S.C. § 112, 1ST PARAGRAPH

A. The Examiner Improperly Introduces Three New Definitions for "Stega-Cipher"

In his Answer on appeal, the Examiner introduces three new definitions of the term "stega-cipher." The Examiner has never articulated that he is applying multiple definitions, and thus, the Examiner's articulating and relying on the new definitions, in effect, changes the rejections of record, thereby prejudicing Appellant. Appellant has not had an opportunity to develop an appeal record for these new definitions, and moreover, to the extent that the introduction of the definitions creates new grounds of rejections, the introduction is

inappropriate. *See* 35 C.F.R. § 1.193(a)(2) ("An Examiner's answer must not include a new ground of rejection").

During prosecution the Appellant was asked to provide a definition for stega-cipher, and Appellant complied. In view of the prosecution history, the only relevant definition of stega-cipher is that which Appellant offered—not the new definitions that have been offered by the Examiner.

The Examiner sets up three definitions for stega-cipher:[1]

> Many interpretations can be applied to the term "stega-cipher". The office has chosen to examine three of these; the material in parentheses is possible claim language for the second clause of claim 25 that incorporates the varied interpretations:
>
> 1) the swaths of specification chosen as support for "stega-cipher" are extensive enough to be non-limiting, effectively making the term's limitations entirely contained within its immediate meaning ("using steganographic and cipher methods to steganographically encode independent information including a digital watermark into the carrier signal");
>
> 2) the specification provides guidelines for the interpretations of "stega-cipher" – the office has interpreted the guidelines for this second scenario to limit the term "stega-cipher" to the selection of an appropriate site for data insertion and the use of a key in the steganographic insertion of material into data ("selecting a portion of the carrier signal that will minimize any perceptible impact of inserting independent information and using a key to steganographically encode independent information including a digital watermark into the carrier signal");
>
> 3) the definition of stega-cipher, as given by applicant in the interview of 04 December 2001, is fully read into the claims (using an algorithm or combination of algorithms to steganographically determine where in the carrier signal data can be hidden 'in plain view' and to use the potential data location information to generate a key that randomly maps the independent information, including a digital watermark, into the carrier signal").

Examiner's Answer at 6-7.

---

[1] It is internally inconsistent for the Examiner to argue on one hand that "on its face, 'stega-cipher' has a definite meaning," (Examiner's Amendment, at 22, para. 2), and yet then offer up three different definitions.

The fact that the Examiner has offered three definitions of "stega-cipher" does not establish that the term is ambiguous, or that Appellant has not sufficiently defined the term in the specification—or even that the term fails to have an established meaning. Moreover, a review of the Examiner's definitions will demonstrate that the Examiner has chosen to introduce new definitions that are inconsistent with each other and with the specification.

The Examiner's first definition is unreasonably broad, and such a broad reading is not consistent with the specification. The Examiner asserts that "the swaths of specification chosen as support for "stega-cipher" are extensive enough to be non-limiting," Examiner's Answer at 6, and thus, the Examiner apparently ignores the specification.[2] The Examiner then rewrites a critical claim limitation of the claims to replace "a stega-cipher" with "steganographic and cipher methods": "using steganographic and cipher methods to steganographically encode independent information including a digital watermark into the carrier signal." Examiner's Answer at 6. The Examiner's redrafting the claims is inappropriate unjustified. While the specification does recite that the stega-cipher is derived from both steganography and cryptography, that does not mean that the Examiner can provide his own definition, especially when, as here, Appellant provided an express definition at the request of the Office.

In drafting the first definition, the Examiner has ignored significant language in the specification. For example, in the "Summary of the Invention," the specification recites that: "The stega-cipher is so named because it uses the steganographic technique of hiding a message in multimedia content, in combination with multiple keys, a concept originating in cryptography. However, instead of using the keys to encrypt the content, the stega-cipher uses these keys to locate the hidden message within the content." Specification, p. 7, ll. 17-20. The Examiner's proposed definition ignores the requirement of a key, and therefore, for at least this reason, the definition is inappropriate and unreasonable. *In re Bass,* 314 F.3d 575, 577 (Fed. Cir. 2002) (citing *In re Yamamoto*, 740 F.2d 1569, 1571 (Fed. Cir. 1984)) ("In examining a patent claim, the PTO must apply the broadest reasonable meaning to the claim language, *taking into account any definitions presented in the specification.*") (emphasis added).

---

[2] It is also inconsistent for the Examiner to assert (in connection with the first definition) that the specification is so broad as to be non-limiting, and yet (in connection with the second definition), the specification is sufficiently precise to provide guidelines to develop a second definition.

While the second definition represents an improvement over the first, the definition is still incomplete. The second definition would define a stega-cipher encoding step as "selecting a portion of the carrier signal that will minimize any perceptible impact of inserting independent information and using a key to steganographically encode independent information including a digital watermark into the carrier signal." For example, the definition is incomplete for at least the reason that the definition does not rely on any "cipher" function as recited in the term "stega-cipher." Thus, the Examiner's second attempt to define stega-cipher is unreasonable, and should not be used.

The third definition represents an improvement over the first and the second, but still, the reliance upon the cipher function is not as precisely stated as in the definition offered by the Appellant. Where, as here, the Appellant has established for the record an express definition for stega-cipher, that definition is the one that should be used.

B. Section 112 Rejections.

Claims 25-63 stand rejected under 35 U.S.C. § 112, first paragraph, as "containing subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention." Office Action dated Dec 10, 2002 at ¶ 20. The Examiner has finally clarified that "the rejection has arisen from use of the term 'stega-cipher'." Examiner's Answer at 22.

As discussed in detail in Appellant's Brief on Appeal, the proper focus of the written description analysis is the claim language and whether the claim language is supported. Brief on Appeal at 5-6. The Examiner concedes that the term "stega-cipher" was present in the specification at the time of filing. Moreover, there is no doubt that there is written support for the term "stega-cipher." Brief on Appeal at 5-8.

As discussed in greater detail below, Examiner improperly focuses on whether support exists in the specification for *his* definitions of stega-cipher, rather than for the claim term itself. Even assuming *arguendo* that the definition of a term is a proper basis for a written description analysis, the Appellant has established for the record an express definition for stega-cipher, and that definition is the one that should be used. Applicant has already fully addressed the support present in the specification for the Applicant's proffered definition of "stega-cipher." Brief on

Appeal at 9-12. Thus, both the claim limitation "stega-cipher" and the Applicant's proffered definition for that term are supported in the specification as originally filed and, accordingly, the rejection for lack of a written description must be reversed.

In particular, the Examiner argues that:

> There is no teaching of using the independent information to form the key. The examiner has interpreted the definition to mean that a key made of a random or pseudo random seed and potential data location information is used to randomly map message data into a carrier signal. The independent information is not used to generate the key.

Examiner's Answer at 7.

Appellant fully addressed this rejection in its Brief on Appeal. *See* Brief on Appeal, pp. 4-12. Accordingly, Appellant will only address the new points raised by the Examiner.

The Examiner argues that Appellant's definition requires that the key must be "based on" the message data. Examiner's Answer at 24-25, paras. 7-8. While this may sound like a matter of semantics, the definition requires only that the "cipher function ... make[] use of ... the message data to generate a key...." It is not entirely understood what the examiner means when he asserts that the key must be "based on" the message data.

Appellant previously explained

> [T]he message data itself is part of the key in that it is placed within the carrier data. In other words, the message and the key are entangled in the embedding process because the key determines where the message bits are located. For example, if one were to compare the original (unwatermarked) carrier signal with the watermarked version, you could determine the locations of the message data (i.e., those portions of the key that identify where data is recorded) as well as the content of the message data (i.e., the message data itself). For this reason, you know the key must be at least as long as the message data—or else the complete message could not be embedded into the carrier signal. In this sense, the message (namely, its length) is utilized in determining a key to embed the message.

Brief on Appeal at 11.

As anyone of skill in the art can testify, and indeed, as Appellant has stated, the key must be *at least* as long as the message, or else, the message cannot be completely encoded. This is inherent in the nature of a key. Without more, this is justification sufficient to conclude that the cipher function makes use of the message data to generate a key.

Moreover, the Examiner erroneously argues that the Appellant's position that "'the message and the key are entangled in the embedding process because the key determines where

the message bits are located'" "directly refutes Applicant's idea that the key is based on the message by highlighting that the two are used together after the key has been created." The Examiner fails to realize that it is possible to use the message data to form the key and then to use the key thus formed to locate the message data within the carrier signal in accordance with the present invention. The cited passage from the Brief on Appeal thus directly supports rather than refutes using the message data to form the key.

The Examiner also asserts that "as Applicant has cited, the length of the primary mask is equal to the sample window size in samples, which teaches away from the idea that the message data is used to generate the key." The two statements are not inconsistent. The referenced language comes from a section of the Specification entitled "Example Embodiment of Encoding and Decoding"—wherein a primary and convolution mask are being used. The section describes in detail how an encoding function will be implemented using a 128 bit primary mask. The section also recites "The encoder proceeds in this manner until a complete copy of the additional information [i.e., the message] has been encoded in the carrier signal." Given that the process encodes one bit at a time, this statement makes clear that the mask being used must be at least as long as the message being encoded. Hence, the Examiner has made an incorrect assumption that one statement teaches away from the other.

The Examiner concedes that the term "stega-cipher" was present in the specification at the time of filing. As discussed in detail in Appellant's Brief on Appeal, there is no doubt that there is written support for the term "stega-cipher" and accordingly, the rejection for lack of a written description must be reversed.

Moreover, even if Appellant is required to show written support for the definition, Applicant has provided adequate support for the definition as shown in its Brief on Appeal, and as discussed above. For this additional reason, the rejection of Claims 25-63 under 35 U.S.C. §112, ¶ 2 must be reversed.

ARGUMENT REGARDING REJECTIONS UNDER 35 U.S.C. §§ 102 AND 103

A. The Examiner Continues to Misread Bender.

In the Office Action, the Examiner pointed out that Bender distinguishes steganography from encryption. Office Action dated Dec. 10, 2002, at ¶ 22. The key distinction lies in whether the perceptible characteristics of the underlying data are changed. Steganography seeks to hide a

message into the underlying data without changing its perceptible characteristics (*i.e.*, "hide the message in plain view"). Encryption seeks to change the underlying data so that it is no longer recognizable.

Examiner's comments regarding Bender and certain other references in his Answer suggest that the Examiner continues to misinterpret the references. In his Answer, the Examiner asserts that Bender "use[s] a key to encrypt watermarks as part of the run-up to inserting the watermark in the signal. Given the teaching of encryption prior to insertion, the characterization of Bender et al. as 'encrypting' watermarks into information with a key is fair." Examiner's Answer at 26. This statement perpetuates the key misapprehension shown in the final rejection: that encrypting the watermark or other data and *then* inserting the encrypted information into the signal is the same as using a stega-cipher to encode a watermark into information. Perhaps recognizing the flaws in this argument, the Examiner claims that "[d]espite the applicability of the examiner's original wording, the first sentences of the 103 rejections have been changed to avoid further confusion." Examiner's Answer at 26. In the few Section 103 rejections over Bender where the Examiner actually changed the language of the rejection,[3] he changed the phrase "encrypting digital watermarks into information with a key" to "encrypting digital watermarks *and placing them* into information with a key."[4]

The claims at issue, however, explicitly require either 1) "using a stega-cipher to steganographically encode independent information including a digital watermark into the carrier signal" (Claim 25 and all claims depending therefrom) or 2) "using a stega-cipher to steganographically decode independent information including a digital watermark from the carrier signal" (Claims 29 and all claims depending therefrom). In either case, it is necessary to

---

[3] In fact, the following rejections under 35 U.S.C. § 103(a) continue to assert that Bender et al teaches "encrypting digital watermarks into information with a key": 1) Claim 36 over Bender in view of Morris, 2) Claim 37 over Bender in view of Powell, 3) Claims 38 an 39 over Bender in view of Braudaway, 4) Claims 40-43 and 46-48 over Bender in view of Schneier, 5) Claims 44, 45, and 49 over Bender and Schneier in view of Cox, 6) Claims 50-51 and 58-61 over Bender and Schneier in view of Barton, 7) Claims 55-57 over Bender in view of Barton. As discussed above and in Appellant's Brief on Appeal, Barton does not disclose "encrypting digital watermarks into information with a key" and each of the foregoing obviousness rejections is improper for failure to disclose each and every limitation of the rejected claims.

[4] See Examiner's Answer at 16-17 (modifying language of Section 103 rejections of Claims 26, 30, and 52-54 over Bender in view of Barton and Claim 34 over Bender).

use a stega-cipher to encode or decode information into a carrier signal, not merely to encrypt information and *then place it* into the carrier signal. For at least this reason, Bender cannot be read to disclose the use of a stega-cipher.

There are other examples wherein the Examiner mischaracterizes Bender. For example, the Examiner asserts that "Scrambling with the random wave is a cipher method." Examiner's Answer at 8. The statement is believed to be made in connection with Figure 2 on page 172, but no "scrambling" is described, nor is any "random wave" described. Similarly, the Examiner recites that "the steganographic function is the selection of the carrier wave." Examiner's Answer at 9. The steganographic function is supposed to say *where* in the carrier signal the watermark will be located. Selection of a carrier wave can hardly be equated to the process of selecting where in the carrier wave the data will be located.

B. <u>The Examiner Appears To Have Misread Powell.</u>

In the Office Action, the Examiner acknowledges the distinction between steganography and encryption, Office Action dated Dec. 10, 2002, at ¶ 22, but the Examiner then appears to overlook the distinctions. The key distinction lies in whether the perceptible characteristics of the underlying data are changed. Steganography seeks to hide a message into the underlying data without changing its perceptible characteristics (*i.e.*, "hide the message in plain view"). Encryption seeks to change the underlying data so that it is no longer recognizable.

In particular, the Examiner's comments regarding Powell and certain other references suggest that the Examiner has not appreciated the distinction between steganography and encryption. In his Answer, the Examiner asserts that:

> EP-Powell uses a key to select alterations to an image as a way to insert an hidden message. In this way, the meaning of the hidden message is concealed. . . . Applicant's error stems largely from a limited conceptualization of encryption, which applicant says "seeks to change the underlying [to be watermarked] data so that it is no longer recognizable." While not incorrect, the preceding fails to recognize that the watermark itself can be encrypted.

Examiner's Answer at 26.

This statement perpetuates the key misapprehension shown in the final rejection: that encrypting the watermark or other data and *then* inserting the encrypted information into the

signal is the same as using a stega-cipher to encode a watermark into information. In the present invention, the key is used to steganographically encode information into a carrier signal such that it is difficult if not impossible to locate the steganographically encoded information without possessing the decode key. Encrypting the information prior to inserting into the carrier signal provides no such protection. Contrary to the Examiner's assertions, encrypting prior to insertion does not involve encrypting *into* a signal as required by the present invention.

As discussed above in the context of Examiner's misreading of Bender, the Examiner's alterations to the language of the Section 103 rejections, as discussed in greater detail below, do not overcome this failure to demonstrate that all of the claimed limitations are present in the cited references. In fact, the changes in language further highlight the Examiner's continuing misreading of Powell.

ARGUMENT REGARDING REJECTIONS UNDER 35 U.S.C. § 102

A. Whether claims 25, 27-29, 31-33, 35, 62 and 63 are unpatentable under 35 U.S.C. § 102 over Bender.

In order for a reference to anticipate a claim, the reference must disclose each and every element of the claimed invention. Independent claim 25 recites, *inter alia*, "using a stega-cipher to steganographically encode independent information including a digital watermark into the carrier signal...." Independent Claim 29 contains similar language. The Section 102 rejections based on Bender are improper for at least the reason that Bender fails to disclose the use of a stega-cipher as required by the rejected claims. The 102 rejections were analyzed in detail in Appellant's initial brief. See Brief on Appeal, pp. 14-16. Accordingly, Appellant will only address the new points raised by the Examiner.

Claims 25, 27-29, 31-33, 35, 62 and 63 stand rejected as allegedly anticipated by Bender. *See* Office Action of December 10, 2002, at ¶22. In the Examiner's Answer, the rejections are discussed in light of the three new definitions. The rejections are not discussed in view of the definition submitted by Applicant. These new rejections are inappropriate. *See* 35 C.F.R. § 1.193(a)(2) ("An Examiner's answer must not include a new ground of rejection").

In his Answer, the Examiner asserts that Applicant relies upon certain features—that are not recited in the claims—to distinguish Bender. Examiner's Answer at 27, para. 11. The Examiner misconstrues Applicant's arguments. Appellant discussed the differences between the stega-cipher of the present invention and the "key" described in Bender. *See* Brief on Appeal at

14-16. Appellant argued that Bender does not disclose the use of a cipher function as required by a stega-cipher of the present invention. Thus, the Examiner is incorrect when he asserts that Appellant relies on limitations not in the claims.

Because Bender fails to disclose a "stega-cipher" as required by claims 25 and 29, the Section 102 rejection of 25 and 29 must be reversed. Moreover, for the same reasons that claims 25 and 29 are patentable over Bender, the claims that depend from claims 25 and 29 are also patentable over Bender. Applicant requests the Board reverse the Section 102 rejection based on Bender, and allow all of the pending claims.

B. Whether claims 25-33, 35-39, 62 and 63 are unpatentable under 35 U.S.C. § 102 over Powell.

In order for a reference to anticipate a claim, the reference must disclose each and every element of the claimed invention. Independent claim 25 recites, *inter alia*, "using a stega-cipher to steganographically encode independent information including a digital watermark into the carrier signal...." Independent Claim 29 contains similar language. The Section 102 rejections based on Powell[5] are improper for at least the reason that Powell fails to disclose the use of a stega-cipher as required by the rejected claims. The 102 rejections were analyzed in detail in Appellant's initial brief. See Brief on Appeal, pp. 16-19. Accordingly, Appellant will only address the new points raised by the Examiner.

Claims 25-33, 35-39, 62 and 63 stand rejected as allegedly anticipated by Powell. *See* Office Action of December 10, 2002, at ¶23. In the Examiner's Answer, the rejections are discussed in light of the three new definitions. The rejections are not discussed in view of the definition submitted by Applicant. These new rejections are inappropriate. *See* 35 C.F.R. § 1.193(a)(2) ("An Examiner's answer must not include a new ground of rejection").

Appellant's Brief on Appeal includes a detailed discussion of how Powell does not disclose the use of a stega-cipher as claimed by the present invention for at least the following reasons: 1) Powell does not disclose the use of a cipher; 2) Powell does not disclose the use of a

---

[5] The Examiner has rejected many of Applicant's claims under 102 using both Bender and Powell. The Examiner attempts to characterize his reliance upon Powell as his "having come across another reference [after an advisory action] that [allegedly] anticipates the independent claims." Examiner's Answer, at 24, para. 6. This characterization is not entirely accurate. Powell was not a newly discovered reference, as the Examiner appears to be asserting. Instead, Powell is related to U.S. Patent No. 5,930,377, which the Examiner cited in an office action dated September 7, 1999.

key to encode or decode; 3) Powell does not embed independent data into a carrier signal; and 4) Powell does not disclose a relationship between the message, signal and key or cipher. Brief on Appeal at 17-19. In response to this argument, the Examiner asserts that the "combination of randomness and the potential signature points constitutes a key that is used to encode." Examiner's Answer at 28. However, the Examiner fails to address how the cited combination acts as a key as required by the rejected claims. Indeed, Powell does not utilize any key—which is why the "image signature" can only be retrieved through the use of the original, unaltered image. Powell, page 5, line 51-page 6, line 9. The present invention's use of keys to encode also permits the use of keys to decode, resulting in a significant practical difference between Powell's teachings and those of the present invention.

The Examiner attempts unsuccessfully to address this very significant practical distinction:

> In the paragraph spanning pages 4 and 5, EP-Powell specifically teaches auditing a signed image with a signature that is "stored by associating the bit value of each signature point together with x-y coordinates of the signature point." The x-y coordinates read on a key. Auditing reads on decoding.

Examiner's Answer at 29. Examiner neglects to mention that the same paragraph of Powell states "In order to allow future auditing of images to determine whether they match the signed image, the signature is stored in a database *in which it is associated with the original image.*" Powell, page 4, lines 57-58 (emphasis added). This passage reinforces—rather than refutes—the fact that Powell requires the use of the original image to retrieve the image signature. Moreover, even if you use the list of x-y coordinates as suggested by the Examiner, one would not be able to get at the encoded information; for this, you would still need the original, unwatermarked original. Quite simply, the Examiner cannot demonstrate how Powell's auditing reads on using a stega-cipher to decode independent information as required by Claim 29 and all claims depending therefrom; this is because one cannot recover the independent information using Bender's key—the precise requirement of Claim 29.

The absence of a key as required by the rejected claims also undercuts Examiner's argument that Powell discloses the relationship "between the message (signature), signal (image), and key is that the key is used to choose points within the image at which to insert the signature." Examiner's Answer at 28. The use of the original, unaltered image to retrieve the "image signature" is antithetical to the concept of a cipher or key as required by the rejected

claims. The Examiner misstates Appellant's argument as a reliance on "the impermissible use of an original carrier signal to decode the independent information", *id.*, a feature the Examiner asserts is not recited in the rejected claims. The relevant claimed feature is "using a stega-cipher to steganographically encode [or decode] independent information including a digital watermark into the carrier signal ...." It is not necessary for Appellant to explicitly claim all of the things that his invention is not. Appellant has claimed the cited limitation and Examiner has failed to show where Powell discloses the required claim limitation.

Examiner also challenges Appellant's assertion that Powell does not embed independent data into the digital image as required by the claimed invention.

> Applicant notes that an original pixel value is changed to a new value that is dependent on the original value. However, this new value is not the signature. Rather, the difference (positive or negative) between the old and new pixel values represents a bit of independent information. In contrast to applicant's assertion that the signature is dependent on the initial pixel value, the representation of the signature in the image uses a difference between the new value and the initial pixel value.

Examiner's Answer at 29. The Examiner's emphasis on the difference between the new and old pixel values is a distinction without a difference. The message content can only be derived by calculating the difference between the new and old pixel values (by using the original unwatermarked signal)—and as Powell teaches, the difference is still a small positive or negative amount relative to the original value (preferably 2-10% of the original value), Powell, page 4, lines 42-48; the information being encoded is thus dependent on the initial value.[6] This makes clear that Powell does not involve the embedding of independent information into a carrier signal, but rather the embedding of information that is dependent upon the initial pixel values. Hence, for this additional reason, Powell fails to disclose encoding or decoding independent information as required by the rejected claims.

Because Powell does not disclose the use of a "stega-cipher" as required by each of the rejected claims, the rejection is improper. With respect to claim 29 (and each of claims 30-33 and 35-38 that depend from claim 29), the Section 102 rejection is improper for the additional reason that Powell does not disclose the use of a key to decode any embedded information. In

---

[6] Contrary to Examiner's assertions, Appellant does not contend that "any change to the carrier signal would make the embedded signal dependent upon the carrier." See Examiner's Answer at 29.

each "preferred" embodiment, Powell requires a comparison of a modified version of an image to the original version of an image, in order to recover any embedded data. This clearly teaches away from using a key. Moreover, since an object of the present invention is to protect the original data, it is undesirable (and, indeed, very risky) to circulate unwatermarked copies of the original data for decoding purposes. Circulation of the decode key, rather than the original data, helps to protect the original data from the risk of unauthorized and untraceable copying. For this additional reason, Applicant's invention teaches away from Powell, and the rejection of claim 29 and its dependencies is improper.

Applicant requests the Board reverse the Section 102 rejection based on Powell, and allow all of the pending claims.

Argument Regarding Rejections Under 35 U.S.C. § 103

In order to "establish a prima facie case of obviousness, three basic criteria must be met." MPEP § 706.02(j). First, there must be some motivation or suggestion to modify the reference or to make the proposed combination. Second, there must be a reasonable expectation of success. "The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on the applicant's disclosure." MPEP § 2142 (citing *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991)). Third, the combined references must teach or suggest all claim limitations.

A. The Examiner has failed to carry his burden to establish a clear and convincing motivation for combining the 103 references.

The Examiner has failed to establish a prima facie case of obviousness to the extent that there is no motivation or suggestion to make the proposed combinations of the references as directed by the Examiner. More particularly, there is no motivation to combine Bender with Schneier and/or Barton. Similarly, there is no motivation to combine Powell with Barton and/or Schneier. The 103 rejections were analyzed in detail in Appellant's initial brief. See Brief on Appeal, pp. 19-31. Accordingly, Appellant will only address the new points raised by the Examiner.

According to the MPEP,

> [i]n order to support a conclusion that the claimed invention is directed to obvious subject matter, either the references must expressly or impliedly suggest the claimed invention or the examiner must present a convincing line of reasoning as to why the artisan would have found the claimed invention obvious in light of the teachings of the references.

MPEP 2142 (citing *Ex parte Clapp*, 277 USPQ 972, 973 (Bd. Pat. App. & Inter. 1985)) (emphasis added). Further, "[w]hen the motivation to combine the teachings of the references is not immediately apparent, it is the duty of the examiner to explain why the combination of teachings is proper." MPEP 2142 (citing *Ex Parte Skinner*, 2 USPQ2d 1788 (Bd. Pat. App. & Inter. 1998)).

The Federal Circuit has recently emphasized the importance of providing evidence of motivation to combine in *Winner Int'l Royalty Corp. v. Ching-Rong Wang*, 202 F.3d 1340, 1348-49 (Fed. Cir. Jan. 27, 2000). "Although a reference need not expressly teach that the disclosure contained therein should be combined with another . . . the showing of combinability, in whatever form, must nevertheless be 'clear and particular.'" *Winner*, 202 F.3d at 1348-49 (citations omitted). Further, the "absence of such a suggestion to combine is *dispositive* in an obviousness determination." *Gambro Lundia AB v. Baxter Healthcare Corp.*, 11 F.3d 1573, 1579 (Fed. Cir. 1997) (emphasis added).

Applicant submits that the Examiner has not satisfied his initial burden of providing "clear and particular" evidence of motivation to combine for any of the proposed combinations of references. Instead, it appears that the Examiner has simply identified references that allegedly disclose the elements of the claim, and has combined them.

In his Answer, the Examiner asserts a post hoc motivation: "In this case, added security would motivate one to incorporate the teachings of Schneier into EP Powell and Bender et al." This conclusory statement, however, does not address Appellant's arguments in the Brief on Appeal and falls short of the required "clear and particular" showing of combinability. *Winner*, 202 F.3d at 1348-49. Even assuming *arguendo* that the references contained all elements of the claimed invention, it is still impermissible to reject a claim as being obvious simply "by locating references which describe various aspects of a patent applicant's invention *without also providing evidence of the motivating force* which would impel one skilled in the art to do what

the patent applicant has done." *Ex parte Levengood*, 28 USPQ2d 1300, 1303 (Bd. Pat. App. & Inter. 1993) (emphasis added).

B. The Examiner has failed to carry his burden to establish a reasonable likelihood of success in combining the 103 references.

Equally important, the Examiner has wholly failed to offer any response to Appellant's argument that there is no likelihood of success. *See* MPEP § 2142 (citing *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991)) ("The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on the applicant's disclosure."). For example, if Bender is trying to achieve steganography, it is not readily apparent how Bender would utilize DES in a steganographic manner. Applying DES to Bender would logically result in an encrypted signal (in contravention of the teachings of Bender). Moreover, using DES to create an encrypted signal is not the same as the claimed invention of using a stega-cipher to steganographically encode a watermark into a carrier signal. Because the Examiner has failed to establish a motivating force and has failed to establish a reasonable likelihood of success, the 103 rejections must be reversed.

C. Whether claims 34, 40-43, 46-48 are unpatentable under 35 U.S.C. § 103 over Powell in view of Schneier.

1. Powell Cannot Properly Be Combined with Schneier.

Applicant's Brief on Appeal provides a detailed discussion of why the combination of Powell and Schneier is inappropriate. Brief on Appeal at 21. Examiner's sole response is that "[i]n this case, added security would motivate one to incorporate the teachings of Schneier into EP Powell and Bender et al." This conclusory statement does not address Appellant's arguments in the Brief on Appeal and falls short of the required "clear and particular" showing of combinability. *Winner*, 202 F.3d at 1348-49.

Because the Examiner has failed to establish a motivating force and has failed to establish a reasonable likelihood of success, the rejection of claims 34, 40-43, and 46-48 based on the combination of Powell and Schneier must be reversed. *See* MPEP § 2142 (citing *In re Vaeck*, 947 F.2d 488 ("The teaching or suggestion to make the claimed combination and the reasonable

expectation of success must both be found in the prior art, and not based on the applicant's disclosure.")).

2. The Combination of Powell and Schneier Does Not Disclose the Claimed Inventions.

The Examiner asserts that claims 34, 40-43, and 46-48 are unpatentable over Powell in view of Schneier.[7] Office Action of December 10, 2002, at ¶ 25. Appellant's Brief on Appeal provides a detailed analysis of how the combination of Powell and Schneier, even if appropriate, would not disclose all of limitations of the rejected claims.

Examiner responds by altering the language of the rejections from "Powell et al. teaches *encrypting digital watermarks into information* with a key," Office Action of December 10, 2002, at ¶ 25 (emphasis added), to "Powell et al. teaches *placing digital signatures into images* with a key." Examiner's Answer at 13 (emphasis added). This alteration of language is significant because it indicates a realization by the Examiner that Powell does not disclose the relevant claim limitation of "using a stega-cipher to steganographically encode [or decode] independent information including a digital watermark into the carrier signal" as required by each of the rejected claims, and establishes that the Examiner is using the teachings of Applicant's invention in an effort to characterize the 103 references.

Examiner further asserts that:

> Applicant mischaracterizes the combination of EP-Powell and Schneier, saying that Schneier would teach encrypting EP-Powell's image. While this combination could be implemented, a more logical joining is the encryption of the signature prior to embedding; in this method, the focus of EP-Powell (a minimally changed image) would be maintained despite the incorporation of Schneier.

Examiner's Answer at 30. Even assuming *arguendo* that sufficient motivation was provided for the combination proposed by the Examiner, that combination would still fail to disclose "using a stega-cipher to steganographically encode [or decode] independent information including a digital watermark into the carrier signal" as discussed in reference to Examiner's misreading of Powell above.

Examiner incorrectly states that "The only claim limitation that applicant cites as being absent from the combination of references is 'mask' set." Examiner's Answer at 31. Contrary to

---

[7] Bruce Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C* (1994).

Examiner's assertion, Appellant also argued that "Powell does not teach 'encrypting digital watermarks into information with a key'" and "the combination fails to disclose the use of a 'stega-cipher' as required by the Claims." Brief on Appeal at 22-23. Examiner has failed to address either of these deficiencies.

The Examiner has simply failed to establish a prima facie case of obviousness. Moreover, the conclusion that the Examiner reaches, namely, "it would have been obvious ... to use masks to protect data" does not appear to be directed to the claim language. The claimed invention requires the use of a stega-cipher to steganographically encode a watermark into a carrier signal. For the simple reason that combining Powell with DES would result in an encrypted image, it is clear that the result is not a steganographically-encoded watermark, as required by *each* of the rejected claims. This practical distinction confirms that the combination cannot yield the claimed invention. Moreover, the combination does not utilize a mask set as required by claims 40-51. For at least these independent reasons, Applicant requests the Board reverse the rejections based on the combination of Powell and Schneier.

D. Whether claim 34 is unpatentable under 35 U.S.C. § 103 over Bender.

The Examiner asserts that Claim 34 is unpatentable over Bender. Appellant's Brief on Appeal pointed out that the Examiner asserts that Claim 34 is obvious in view of Bender, yet the basis provided for this assertion does not appear to be related to Claim 34. *See* Office Action of December 10, 2002, at ¶ 31. Examiner fails to address this deficiency in his Answer. The only alterations made to the rejection was a change from "Bender et al. teaches *encrypting digital watermarks into information* with a key," Office Action of December 10, 2002, at ¶ 31 (emphasis added), to "Bender et al. teaches encrypting digital watermarks *and placing them into* images with a key." Examiner's Answer at 13 (emphasis added). This alteration of language is significant because it indicates a realization by the Examiner that Bender does not disclose the relevant claim limitation of "using a stega-cipher to steganographically *encode [or decode]* independent information including a digital watermark *into* the carrier signal" as required by each of the rejected claims. Examiner thus has failed to establish a prima facie case of obviousness. See MPEP 706.02(j) (the combined references must teach or suggest all claim limitations).

E. Whether claims 40-43 and 46-48 are unpatentable under 35 U.S.C. § 103 over Bender in view of Schneier.

1. Bender Cannot Properly Be Combined with Schneier.

Applicant's Brief on Appeal provides a detailed discussion of why the combination of Bender and Schneier is inappropriate. Brief on Appeal at 21. Examiner's sole response is that "[i]n this case, added security would motivate one to incorporate the teachings of Schneier into EP Powell and Bender et al." Examiner's Answer at 30. This conclusory statement does not address Appellant's arguments in the Brief on Appeal and falls short of the required "clear and particular" showing of combinability. *Winner*, 202 F.3d at 1348-49.

Because the Examiner has failed to establish a motivating force and has failed to establish a reasonable likelihood of success, the rejection of claims 40-43 and 46-48 based on the combination of Bender and Schneier must be reversed. *See* MPEP § 2142 (citing *In re Vaeck*, 947 F.2d 488 ("The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on the applicant's disclosure.")).

2. The Combination of Bender and Schneier Does Not Disclose the Claimed Inventions.

Examiner rejects claims 40-43 and 46-48 as unpatentable over Bender in view of Schneier. *See* Office Action dated Dec. 10, 2002, at ¶ 35. Appellant's Brief on Appeal provides a detailed analysis of how the combination of Bender and Schneier, even if appropriate, would not disclose all of limitations of the rejected claims. Brief on Appeal at 25-26.

Examiner responds that "Applicant's comments with respect to the combination of Bender et al. and Schneier are flawed in the same manner as applicant's analysis of the combination of Schneier and EP-Powell." Examiner's Answer at 31. It is not entirely clear, but Examiner appears to be referring to the following passage:

> Applicant mischaracterizes the combination of EP-Powell and Schneier, saying that Schneier would teach encrypting EP-Powell's image. While this combination could be implemented, a more logical joining is the encryption of the signature prior to embedding; in this method, the focus of EP-Powell (a minimally changed image) would be maintained despite the incorporation of Schneier.

Examiner's Answer at 30. Even assuming *arguendo* that sufficient motivation was provided for the combination proposed by the Examiner, that combination would still fail to disclose "using a stega-cipher to steganographically encode [or decode] independent information including a digital watermark into the carrier signal" as discussed in reference to Examiner's misreading of Powell above.

Claims 40-51 rely on the use of a "mask set." Because Schneier fails to disclose or suggest the use of a mask set as disclosed in the claims (whether alone or in combination with the other references), and even fails to disclose the use of a stega-cipher, the rejections of claims 40-43 and 46-48 must be reversed. *See* MPEP 706.02(j) (the combined references must teach or suggest all claim limitations).

Claims 40-43 (which depend from independent claim 25) and claims 46-48 (which depend from independent claim 29) are also patentable over the combination because the combination fails to disclose the use of a "stega-cipher" as required by the claims. For at least this additional reason, the Examiner has failed to establish a prima facie case of obviousness, and thus the rejections of claims 40-43 and 46-48 must be reversed. *See* MPEP 706.02(j) (the combined references must teach or suggest all claim limitations).

F. Whether claims 52-57 are unpatentable under 35 U.S.C. § 103 over Powell in view of Barton.[8]

1. Powell Cannot Properly Be Combined with Barton.

Appellant's Brief on Appeal presents detailed support for why Powell and Barton cannot be properly combined and why it is not readily apparent that there is a reasonable likelihood of success in combining the techniques of Barton with the techniques of Powell, at least as suggested by Examiner. Examiner's sole response in his Answer is "Barton's teachings provide assurances that data is correctly ordered and all present (lines 30-33 of column 4), which is beneficial and hence a motivation to employ the teachings of Barton in EP Powell and Bender et al." Examiner's Answer at 30. This conclusory statement does not address Appellant's arguments in the Brief on Appeal and falls short of the required "clear and particular" showing of

[8] U.S. Patent No. 5,912,972.

combinability. *Winner*, 202 F.3d at 1348-49. Simply pointing out the claimed benefits of one reference provides no motivation for why one skilled in the art would have selected these components for combination in the manner claimed. *See In re Kotzab*, 217 F.3d, 1371 (Fed. Cir. 2000) ("particular findings must be made as to the reason the skilled artisan, with no knowledge of the claimed invention, would have selected these components for combination in the manner claimed"). Thus, there is no motivation for combining Powell and Barton, and the rejections of claims 52-57 based on the combination of Powell and Barton must be reversed.

2. The Combination of Powell and Barton Does Not Disclose the Claimed Inventions.

The Examiner asserts that claims 52-57 are unpatentable over Powell in view of Barton. Office Action dated Dec. 10, 2002, at ¶¶ 28-29. Appellant's Brief on Appeal provides a detailed analysis of how the combination of Powell and Barton, even if appropriate, would not disclose all limitations of the rejected claims. Brief on Appeal at 27-29.

With respect to claims 52-54, Examiner responds by altering the language of the rejection from "Powell et al. teach *encrypting digital watermarks into information*," Office Action of December 10, 2002, at ¶ 28 (emphasis added), to "Powell et al. teach *embedding* digital *signatures* into information." Examiner's Answer at 15 (emphasis added). With respect to Claims 55-57, Examiner changes the language of the rejection from "Powell et al. teach *encrypting digital watermarks into information with a key*," Office Action of December 10, 2002, at ¶ 29 (emphasis added), to "Powell et al. teach *embedding* digital *signatures as* watermarks into information with a key." Examiner's Answer at 13 (emphasis added). These alterations of language are significant because they indicates a realization by the Examiner that Powell does not disclose the relevant claim limitation of "using a stega-cipher to steganographically encode [or decode] independent information including a digital watermark into the carrier signal" as required by each of the rejected claims.

As discussed above, Powell does not teach "encrypting digital watermarks into information with a key," and furthermore, does not teach the use of a stega-cipher for steganographically encoding watermarks into a carrier signal. The addition of Barton does not cure this shortcoming. For at least this reason, the combination does not yield the claimed invention, and accordingly, the 103 rejection of claims 52-57 must be reversed.

Claims 52-57 are allowable for the additional reason that the combination of Powell and Barton fails to yield another aspect of claim 52. Claim 52 relates to "adding unique data to each individual watermark, rendering it distinct from any other watermark in the same sample stream." Claim 52 requires that multiple watermarks exist in the same sample stream. Applicant noted in his Brief on Appeal that the Examiner has not established where Powell (or Barton) teaches the use of multiple watermarks. Brief on Appeal at 28. Examiner responds that "Barton clearly teaches different and hence multiple watermarks in lines 30-33 of Column 4 by teaching sequence numbers added to frames. Examiner's Answer at 32. As discussed in the brief on Appeal, Barton suggests that where the *underlying data* comprises sequential data such as video frames (for example, where the digital blocks represent video frames), the meta data being added can include frame numbers to indicate the sequence order. It would appear that the Examiner's argument has assumed that the meta-data represents a watermark (because it represents independent data provided by the user). The Examiner, however, is relying on the insertion of sequence information that directly relates to the *underlying data*. Thus, at best the Examiner's citation of Barton suggests that unique information about the *underlying data* can be added to the meta data to provide information about the *underlying data.* Claim 52 is directed to the *unique identification of multiple watermarks* that may be embedded into underlying data. Barton, at best, appears to teach the unique identification of the underlying data. The motivation for marking Barton's underlying data is based upon the purpose of the underlying data (*e.g.*, video frames). This motivation does not suggest any need or desire to uniquely mark the data that is being embedded into the underlying data. So, even assuming a motivation for combining Barton and Powell, the combination still does not disclose the invention of Claim 52, and therefore claim 52, and claims 53-57 that depend from claim 52, are not obvious. For at least this additional reason, the Board must reverse the rejection of Claims 52-57.

G. Whether claims 26, 30, and 52-57 are unpatentable under 35 U.S.C. § 103 over Bender in view of Barton.

Examiner rejects claims 26, 30, 52-54, and 55-57 as unpatentable over Bender in view of Barton. *See* Office Action dated Dec. 10, 2002, at ¶¶ 30 and 38. Appellant's Brief on Appeal provides a detailed analysis of how the combination of Bender and Barton would not disclose all limitations of the rejected claims. Brief on Appeal at 29-31.

With respect to claims 52-54, Examiner responds by altering the language of the rejection from "Bender et al. teaches *encrypting digital watermarks into information with a key*," Office Action of December 10, 2002, at ¶ 30 (emphasis added), to "Bender et al. teach encrypting digital watermarks *and placing them* into information with a key." Examiner's Answer at 16 (emphasis added). This alteration of language is significant because it indicates a realization by the Examiner that Powell does not disclose the relevant claim limitation of "using a stega-cipher to steganographically encode [or decode] independent information including a digital watermark into the carrier signal" as required by each of the rejected claims.

For the same reasons as described above for the combination of Powell and Barton, Claims 52-57 are allowable for at least the reason that the combination of Bender and Barton fails to yield the step of "adding unique data to each individual watermark, rendering it distinct from any other watermark in the same sample stream."

As discussed above, Bender does not teach the use of a stega-cipher for steganographically encoding watermarks into a carrier signal. The addition of Barton does not cure this shortcoming. For at least this additional reason, the combination does not yield the claimed invention, and accordingly, the Section 103 rejection of claims 26, 30, 52-54, and 55-57 must be reversed.

CONCLUSION

For the reasons set forth above, Appellant respectfully requests that the Board reverse the final judgment of the Examiner and instruct the Examiner to issue a notice of allowance for the Claims 25-63 as last amended.

Respectfully submitted,

WILEY REIN & FIELDING LLP

Date: December 1, 2003

By: Floyd B Chapman

Floyd B. Chapman Reg. No. 40,555

WILEY REIN & FIELDING LLP
Attn: Patent Administration
1776 K Street, N.W.
Washington, D.C. 20006
Telephone: 202.719.7000
Facsimile: 202.719.7049